IN THE CLAIMS

1. (Previously Presented) A method for handling on a wireless mobile communication device a secure message to be sent from the wireless mobile communication device to a recipient, comprising the steps of:

receiving data at the wireless mobile communication device about a security key associated with the recipient;

using the received data to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient;

wherein an issue exists due to the validity check;

determining a reason for the validity check issue;

wherein the reason for the validity check issue is provided via a user interface on the mobile device;

wherein a message is provided via the user interface indicating that a problem exists with respect to sending the secure message to the recipient in addition to indicating the reason related to the problem.

2. (Cancelled)

3. (Previously Presented) The method of claim 1, further comprising the step of resolving the validity check issue associated with using the security key through use of the information provided in the validity check reason, wherein the secure message is sent after resolution of the validity check issue by the user.

4. (Previously Presented) The method of claim 1, wherein the security key is a public key, wherein a user composes the secure message, wherein the composed message is to be encrypted using the recipient's public key.

5. (Previously Presented) The method of claim 4, further comprising the steps of:

creating a list of all recipients for the composed message;

receiving data about the recipients' public keys that includes certificate information associated with the recipients; and

performing the validity check with respect to the certificate information associated with the recipients.

6. (Previously Presented) The method of claim 1, further comprising the steps of:

determining whether a certificate for an intended recipient can be located;

providing as a validity check reason that the intended recipient's certificate was not located.

7. (Previously Presented) The method of claim 6 further comprising the step of removing a recipient whose certificate was not located before sending a secure message to another recipient.

8. (Previously Presented) The method of claim 6 further comprising the step of canceling sending the message to a recipient whose certificate was not located.

9. (Previously Presented) The method of claim 6, further comprising the step of:

determining whether the certificate for the intended recipient is locally available on the mobile device.

10. (Previously Presented) The method of claim 6, further comprising the step of:

determining whether the certificate for the intended recipient is remotely available.

11. (Previously Presented) The method of claim 5, further comprising the step of collating certificates that correspond to the recipients before performing the validity check.

12. (Previously Presented) The method of claim 6, wherein the message is to be encrypted using a Secure Multipurpose Internet Mail Extensions (S/MIME) scheme or a Pretty Good Privacy (PGP) scheme.

13. (Previously Presented) The method of claim 1, wherein the received data about the security key associated with the recipient includes whether a recipient's certificate is permitted to be used;

wherein the validity check issue indicates that the recipient's certificate is not permitted to be used.

14. (Previously Presented) The method of claim 13, wherein the data about whether the recipient's certificate is permitted to be used is based on a usage field contained in the certificate.

15. (Previously Presented) The method of claim 13, wherein the data about whether the recipient's certificate is permitted to be used is based on a control file installed on the mobile device that specifies which certificates are allowed to be used.

16. (Previously Presented) The method of claim 1, wherein the issue involves a validity check failure, said method further comprising the step of providing the reason of the validity check failure to the user interface on the mobile device.

17. (Previously Presented) The method of claim 1, wherein the received data about the security key associated with the recipient includes strength of the recipient's certificate; and

wherein the validity check issue is directed to whether the recipient's certificate is permitted to be used based upon the strength of the recipient's certificate.

18. (Previously Presented) The method of claim 1, wherein the received data about the security key associated with the recipient includes whether the recipient's certificate is trusted, and wherein a decision to include a recipient for a secure message is based upon whether the recipient's certificate is trusted.

19. (Previously Presented) The method of claim 1, wherein the received data about the security key associated with the recipient includes validity and revocation status of a recipient's certificate, and wherein a decision to include the recipient for the secure message is based upon the validity and revocation status of the recipient's certificate.

20. (Previously Presented) The method of claim 1, wherein the message is sent to the recipient despite notification of the validity check issue.

21. (Original) The method of claim 1, wherein means for providing a wireless network and means for providing a message server are used to transmit the secure message from the mobile device.

22. (Original) The method of claim 1, wherein the mobile device is a handheld wireless mobile communications device or a personal digital assistant (PDA).

23. (Canceled)

24. (Canceled)

25. (Previously Presented) An apparatus for handling on an electronic device a secure message to be sent from the electronic device to a recipient, comprising:

a secure message processing module for use with a messaging client that sends electronic messages to recipients;

wherein the secure message processing module receives data about a security key associated with the recipient;

wherein the secure message processing module uses the received data to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient;

wherein an issue exists based upon the validity check;

wherein the secure message processing module is configured to determine a reason for the validity check issue; and

wherein the secure message processing module provides the reason for the validity check issue via a user interface of the electronic device;

wherein a message is provided via the user interface indicating that a problem exists with respect to sending the secure message to the recipient in addition to indicating the reason related to the problem.

26. (Cancelled)

27. (Previously Presented) A computer-readable storage medium encoded with instructions that cause a processor to perform a method for handling on a wireless mobile communication device a secure message that is to be sent from the wireless mobile communication device to a recipient, said method comprising:

receiving data at the wireless mobile communication device about a security key associated with the recipient;

using the received data to perform a validity check with respect to using the security key associated with the message recipient to send a secure message to the recipient;

wherein an issue exists due to the validity check;

determining a reason for the validity check issue;

wherein the reason for the validity check issue is provided via a user interface on the mobile device;

wherein a message is provided via the user interface indicating that a problem exists with respect to sending the secure message to the recipient in addition to indicating the reason related to the problem.

28. (New) A method for handling on a wireless mobile communication device a secure message to be sent from the wireless mobile communication device to a recipient, comprising the steps of:

receiving data at the wireless mobile communication device about a security key associated with the recipient;

using the received data to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient;

wherein an issue exists due to the validity check;

determining a reason for the validity check issue;

wherein the reason for the validity check issue is provided via a user interface on the mobile device; and

resolving the validity check issue associated with using the security key through use of the information provided in the validity check reason, wherein the secure message is sent after resolution of the validity check issue by the user.

29. (New) The method of claim 28, wherein a message is provided via the user interface indicating that a problem exists with respect to sending the secure message to the recipient in addition to indicating the reason related to the problem.

30. (New) The method of claim 28, wherein the security key is a public key, wherein a user composes the secure message, wherein the composed message is to be encrypted using the recipient's public key.

31. (New) The method of claim 30, further comprising the steps of:

creating a list of all recipients for the composed message;

receiving data about the recipients' public keys that includes certificate information associated with the recipients; and

performing the validity check with respect to the certificate information associated with the recipients.

32. (New) The method of claim 28, further comprising the steps of:

determining whether a certificate for an intended recipient can be located;

providing as a validity check reason that the intended recipient's certificate was not located.

33. (New) The method of claim 32 further comprising the step of removing a recipient whose certificate was not located before sending a secure message to another recipient.

34. (New) The method of claim 32 further comprising the step of canceling sending the message to a recipient whose certificate was not located.

35. (New) The method of claim 32, further comprising the step of:

determining whether the certificate for the intended recipient is locally available on the mobile device.

36. (New) The method of claim 32, further comprising the step of:

determining whether the certificate for the intended recipient is remotely available.

37. (New) The method of claim 31, further comprising the step of collating certificates that correspond to the recipients before performing the validity check.

38. (New) The method of claim 32, wherein the message is to be encrypted using a Secure Multipurpose Internet Mail Extensions (S/MIME) scheme or a Pretty Good Privacy (PGP) scheme.

39. (New) The method of claim 28, wherein the received data about the security key associated with the recipient includes whether a recipient's certificate is permitted to be used;

wherein the validity check issue indicates that the recipient's certificate is not permitted to be used.

40. (New) The method of claim 39, wherein the data about whether the recipient's certificate is permitted to be used is based on a usage field contained in the certificate.

41. (New) The method of claim 39, wherein the data about whether the recipient's certificate is permitted to be used is based on a control file installed on the mobile device that specifies which certificates are allowed to be used.

42. (New) The method of claim 28, wherein the issue involves a validity check failure, said method further comprising the step of providing the reason of the validity check failure to the user interface on the mobile device.

43. (New) The method of claim 28, wherein the received data about the security key associated with the recipient includes strength of the recipient's certificate; and

wherein the validity check issue is directed to whether the recipient's certificate is permitted to be used based upon the strength of the recipient's certificate.

44. (New) The method of claim 28, wherein the received data about the security key associated with the recipient includes whether the recipient's certificate is trusted, and wherein a decision to include a recipient for a secure message is based upon whether the recipient's certificate is trusted.

45. (New) The method of claim 28, wherein the received data about the security key associated with the recipient includes validity and revocation status of a recipient's certificate, and wherein a decision to include the recipient for the secure message is based upon the validity and revocation status of the recipient's certificate.

46. (New) The method of claim 28, wherein the message is sent to the recipient despite notification of the validity check issue.

47. (New) The method of claim 28, wherein means for providing a wireless network and means for providing a message server are used to transmit the secure message from the mobile device.

48. (New) The method of claim 28, wherein the mobile device is a handheld wireless mobile communications device or a personal digital assistant (PDA).

49. (New) An apparatus for handling on an electronic device a secure message to be sent from the electronic device to a recipient, comprising:

a secure message processing module for use with a messaging client that sends electronic messages to recipients;

wherein the secure message processing module receives data about a security key associated with the recipient;

wherein the secure message processing module uses the received data to perform a validity check with respect to using the security key associated with the recipient to send a secure message to the recipient;

wherein an issue exists based upon the validity check;

wherein the secure message processing module is configured to determine a reason for the validity check issue; and

wherein the secure message processing module provides the reason for the validity check issue via a user interface of the electronic device; and

wherein the secure message processing module resolves the validity check issue associated with using the security key through use of the information provided in the validity check reason, wherein the secure message is sent after resolution of the validity check issue by the user.

50. (New) A computer-readable storage medium encoded with instructions that cause a processor to perform a method for handling on a wireless mobile communication device a secure message that is to be sent from the wireless mobile communication device to a recipient, said method comprising:

receiving data at the wireless mobile communication device about a security key associated with the recipient;

using the received data to perform a validity check with respect to using the security key associated with the message recipient to send a secure message to the recipient;

wherein an issue exists due to the validity check;

determining a reason for the validity check issue;

wherein the reason for the validity check issue is provided via a user interface on the mobile device; and

resolving the validity check issue associated with using the security key through use of the information provided in the validity check reason, wherein the secure message is sent after resolution of the validity check issue by the user.